

REMARKS

Claims 1-3, 19, and 23-40 are pending in the present application. By this Response, claims 1, 27, and 33 are amended for clarification by removing the term "may be" and to further clarify that the object classes are part of an object model in an object oriented programming language. Support for these amendments may be found at least at page 7, lines 24-28. It is believed that these amendments to claims 1, 27, and 33 do not change the scope of the claims since the claims already utilized the term object classes which is defined at page 7, lines 24-28 as being a definition of objects in an object model in an object oriented programming language and thus, reading the unamended claims in light of the specification would necessitate the interpretation of the term "object classes" as they are now explicitly defined in the claims.

Claim 33 is amended to recite "a computer program product comprising a computer-usable *storage* medium having computer-executable instructions *stored thereon* for handling personally identifiable information..." in order to address the 35 U.S.C. § 101 issues raised by the Office Action. Support for this amendment may be found at least at page 34 of the present specification and Figure 1, elements 114 or 116 as non-limiting examples of such storage media.

In addition, claim 3 is amended to recite additional features of the present invention. Support for the addition of features to claim 3 may be found at least page 10, line 17 to page 11, line 21. Claims 39-40 are added to recite additional features of the present invention. Support for the addition of claims 39-40 may be found at least at page 20, lines 11-29. No new matter has been added by any of the above amendments. Reconsideration of the claims is respectfully requested in view of the above amendments and the following remarks.

I. Telephone Interview

A telephone interview was not able to be scheduled prior to the response due date. Therefore, Applicants respectfully request that the Examiner contact Applicants' representative to discuss this application prior to taking any further action on this case.

II. Objection to the Specification

The Office Action objects to the specification stating that the Abstract needs to be 150 words or less and certain language in the Abstract referencing "the invention" should be removed. By this Response, the Abstract is amended to conform with these requirements.

In addition, the Office Action objects to the specification stating that a hyperlink on page 8, line 15 needs to be deleted from the specification. By this Response, the hyperlink on page 8, line 15 is deleted as requested. Accordingly, Applicants respectfully request withdrawal of the objection to the specification.

III. Rejection under 35 U.S.C. 112, Second Paragraph

The Office Action rejects claims 1, 27, and 33 under 35 U.S.C. § 112, second paragraph as being allegedly indefinite. Specifically, the Office Action rejects these claims for including the phrase "may be." By this Response, claims 1, 27, and 33 are amended to remove the term "may be" and replace it with the word "is." Thus, Applicants respectfully request withdrawal of the rejection of claims 1, 27, and 33 under 35 U.S.C. § 112, second paragraph.

IV. Rejection under 35 U.S.C. § 101

The Office Action rejects claims 33-38 under 35 U.S.C. § 101 as being allegedly directed to non-statutory subject matter. By this Response, claim 33 is amended to clearly direct the claim to non-carrier wave, signal, or transmission media by reciting a computer-useable *storage* medium having the instructions *stored thereon*. Thus, Applicants respectfully submit that claims 33-38 are directed to statutory subject matter and respectfully request withdrawal of the rejection of claims 33-38 under 35 U.S.C. § 101.

V. Rejection under 35 U.S.C. § 102(e)

The Office Action rejects claims 1-2, 23-24, 27, 29-30, 33, and 35-36 under 35 U.S.C. § 102(e) as being allegedly anticipated by King (U.S. Patent No. 7,093,286). This rejection is respectfully traversed.

Claim 1, which is representative of the other rejected independent claims 27 and 33 with regard to similarly recited subject matter, reads as follows:

1. A method, in a data processing system, for handling personally identifiable information, said method comprising:
 - providing, in a computer, ***a first set of object classes, of an object model in an object oriented programming language, representing active entities in an information-handling process;***
 - providing, in said computer, ***a second object class, of the object model, representing personally identifiable information and associated rules in said information-handling process;*** and
 - processing transactions, in the data processing system, involving said personally identifiable information, using said computer and said ***first set of object classes and said second object class of the object model***, so as to enforce a privacy policy, wherein
 - said rules define if and how ***said personally identifiable information is provided, by a first data user that previously requested the personally identifiable information from an active entity that is personally identifiable by the personally identifiable information, to a second data user that requests said personally identifiable information from the first data user.*** (emphasis added)

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. In re Bond, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. In re Lowry, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. Kalman v. Kimberly-Clark Corp., 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). Applicants respectfully submit that King does not identically show every element of the claimed invention arranged as

they are in the claims. Specifically, King does not teach the features of claim 1 emphasized above, or the similar features found in the other rejected independent claims.

King is directed to a mechanism for communicating sensitive information in a wireless communication system. With the mechanism of King, the exchange, as well as the use and nature, of sensitive information released can be governed by one or more privacy agreements established between principle parties, namely a client device and a content server (column 5, lines 6-9). A proxy server device is used as a trusted third party such that, once a privacy agreement is established between the client and the content server, the content server can obtain sensitive information (which in the examples of King is location information) from either the client or the proxy server (column 5, lines 24-28). The sensitive information is provided from the client to the proxy server in requests sent by the client device or, alternatively, the proxy server can ask for the information from the client device (column 6, lines 50-58).

The client may send a request to the proxy server which then forwards the request on to the content server. The content server may then request sensitive information from the proxy server. The proxy server then determines whether there is an existing privacy agreement between the client and the content server. If not, then the client and the content server must negotiate one prior to the exchange of the sensitive information (column 7, lines 20-35). A privacy manager on the proxy server may act as a negotiating agent between the client and the content server (column 9, lines 37-49).

Thus, with King, as long as a privacy agreement exists between a client and a server, then a third party entity, e.g., the proxy server, may provide sensitive information to the server on behalf of the client. If a privacy agreement does not exist between the client and the server, then one must be negotiated before the release of the sensitive information is allowed to happen.

It should first be noted that nowhere in King is there any mention of an object model being provided in an object oriented programming language. Furthermore, nowhere in King is there any teaching regarding such an object model that includes a first set of object classes representing active entities in an information-handling process, a second object class representing personally identifiable information and associated rules in the information handling process, or processing transactions using the first and second object

classes in such an object model. King does mention "Handset Location Object (HLO)", "Network Location Object (NLO)", and an "Absolute Location Object (ALO)", but the term "object" in this context is being used generically to mean data; the term is not being used to refer to an object model in an object oriented programming language. However, even if the term "object" were being used to refer to objects in an object oriented programming language model, *arguendo*, at most these objects would represent sensitive information. There still would not be any mention of the particular objects set forth in claim 1, or the manner by which these objects in claim 1 are utilized to process transactions.

A key difference between King and the presently claimed invention as recited in claim 1 is that the privacy agreement in King is an agreement between the parties, i.e. the client and the content server, and is not tied to the particular sensitive information that is being communicated. That is, in the presently claimed invention, the rules, which specify if and how personally identifiable information, about an active entity, may be provided by a first data user to a second data user, are tied to the actual personally identifiable information by being defined in a "second object class" of the object model, the second object class representing the ***personally identifiable information and associated rules***.

In King, the privacy agreement exists, or does not exist, independent of the sensitive information. This is clear in that King allows for the possibility that a server may request sensitive information from a proxy server and there may not be an existing privacy agreement to govern the transfer of such sensitive information and thus, one will be negotiated. Such a situation will not arise in the presently claimed invention since the personally identifiable information is tied to the rules governing its dissemination, by defining both the personally identifiable information and its associated rules in the second object class. Such a capability is not provided in the mechanism of King. In fact, as noted above, King does not even teach object classes of an object model in an object oriented programming language and thus, cannot teach such an object class representing the personally identifiable information and its associated rules.

Since King does not teach object classes of an object model in an object oriented programming language, let alone the specific object classes recited in claim 1, King cannot teach to process transactions using such object classes. To the contrary, King only looks to

see if a privacy agreement exists between the client and the content server and if one does exist, then the sensitive information is allowed to be transmitted to the content server. King does not use a first set of object classes representing active entities in an information handling process, and a second object class representing personally identifiable information and its associated rules, to process transactions.

Moreover, the privacy agreement between the client and the content server in King does not define if and how the proxy server is able to provide the sensitive data, requested by the proxy server, to the content server that requested the sensitive data from the proxy server. To the contrary, the agreement between the client and the content server is merely an agreement that states that the content server is permitted to receive sensitive information about the client. It is not specifically directed to if and how the proxy server provides such information to the content server. Thus, the privacy agreement in King is not equivalent to the rules that define if and how *said personally identifiable information is provided, by a first data user that previously requested the personally identifiable information from an active entity that is personally identifiable by the personally identifiable information, to a second data user that requests said personally identifiable information from the first data user.*

For at least the reasons set forth above, Applicants respectfully submit that King does not teach each and every feature of independent claim 1 as is required under 35 U.S.C. § 102(e), or the similar features found in the other rejected independent claims 27 and 33. At least by virtue of their dependency on claims 1, 27, and 33, respectively, King does not teach each and every feature of dependent claims 2, 23-24, 29-30, and 35-36. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1-2, 23-24, 27, 29-30, 33, and 35-36 under 35 U.S.C. § 102(e).

In addition to the above, King does not teach the specific features of dependent claims 2, 23-24, 29-30, and 35-36. For example, with regard to claim 2, King does not teach that a first set of object classes includes one or more object classes representing parties, selected from the group consisting of: a data user object class, a data subject object class, a guardian object class, and a privacy authority object class. In another example, with regard to claims 23, 29 and 35, King does not teach that a privacy policy is associated with the personally identifiable information and defined by the rules, and is

enforced against one or more active entities represented by the first set of object classes, and wherein each of the one or more active entities represented by the first set of object classes is a human being or legal entity. As mentioned above, King does not even mention object classes of an object model, let alone any one of these specific object classes set forth in these claims or the use of such object classes. Thus, King does not identically teach the features of claims 2 and 23 as is required under 35 U.S.C. § 102(e).

As another example, with regard to claims 24, 30 and 36, King does not teach a first active entity *represented by a first object class in said first set of object classes* is said *first data user* that previously requested said personally identifiable information from *said data subject that is a second active entity represented by a second object class in said first set of object classes*, and *a third active entity represented by a third object class in said first set of object classes* is said *second data user* that requests said personally identifiable information from said first data user. Again, King does not teach any object classes at all, let alone the specific object classes recited in the claims. Nowhere in King is there any teaching to represent the client, the proxy server, and the content server as objects in a first set of object classes that represent active entities. Nowhere in King is there any teaching to use such object classes, along with another object class representing the sensitive information and its associated rules, to process transactions. King only teaches to establish a privacy agreement between the client and the content server, and to have the proxy server ensure that such an agreement is in place before transmitting the sensitive information; otherwise an agreement must be negotiated before transmitting the sensitive information. King does not teach the specific features of claim 24 as is required under 35 U.S.C. § 102(e).

Thus, in addition to their dependency, claims 2, 23-24, 29-30, and 35-36 are distinguished over King based on the specific features recited in these claims.

VI. Rejection under 35 U.S.C. § 103(a) Based on King and Tolopka

The Office Action rejects claim 3 under 35 U.S.C. § 103(a) as being allegedly unpatentable over King (U.S. Patent No. 7,093,286) in view of Tolopka (U.S. Patent No. 6,044,349). This rejection is respectfully traversed for at least the same reasons as set

forth above with regard to the 35 U.S.C. § 102(e) rejection based on King. That is, King does not teach or render obvious the features discussed above. Moreover, Tolopka does not provide any teaching or technical rationale to implement the features missing from King as noted above.

Amended claim 3 reads as follows:

3. The method of claim 1, wherein said second object class, having said rules associated with said data, ***represents a filled paper form, including both collected data, collected from the active entity and including the personally identifiable information, and rules regarding said collected data specifying if and how the collected data is provided to the second data user, wherein the second data user sends an empty form including a policy to the first data user requesting the personally identifiable information, and wherein the first data user checks the policy included with the empty form to determine if disclosure of the personally identifiable information is permitted based on the policy included with the empty form and the rules regarding the collected data.***
(emphasis added)

Neither King nor Tolopka, either alone or in combination, teach or render obvious at least those features of claim 3 emphasized above.

Tolopka is directed to a portable storage medium to store data and provide access to information from an information dissemination system (IDS). The storage medium can store one or more location/key pairs. Each of the location/key pairs designates a particular IDS location as well as an access key to the particular IDS location. The storage medium can also store a plurality of information units. The information units are categorized into levels of information categories with at least one information category per level and at least one information unit per information category. Levels of information categories can be individually accessed and categories of information units within levels can be selectively downloaded.

Thus, Tolopka is only concerned with what access a particular information seeking system has to an IDS, and controls this access based on a key providing on a smart card. The key and smart card in Tolopka operate in a similar manner as Access Control Lists (ACLs) in that they only control access by that particular subject, or information seeking system, to a particular object. They do not have anything to do with

controlling how the information seeking system may then send that information to another information seeking system. Moreover, the key and smart card mechanism of Tolopka does not provide any teaching, or even suggestion, regarding a filled paper form, including both collected data, collected from the active entity and including the personally identifiable information, and rules regarding said collected data specifying if and how the collected data is provided to the second data user. Tolopka at most teaches adding labels and data to a table.

The Office Action points to column 6, lines 326-52 of Tolopka as allegedly teaching objects that may represent paper-filled forms. Applicants respectfully submit that this section of Tolopka states that the user may manually type information with a text editor or other application and download it to the storage medium such that user entered labels, and apparently the data, may be added to the table shown in Figure 2, which is a depiction of information categories and information units stored on the storage medium (see Tolopka, Brief Description of the Drawings). Simply because the user can add labels and data to a data structure, which is depicted as a table in Figure 2, does not mean that Tolopka teaches an object class having rules associated with data that represents a filled paper form including both collected data and rules regarding the collected data, as recited in claim 3. The table in Figure 2 of Tolopka is not an object class representing a filled paper form and furthermore, does not include both collected data and rules regarding the collected data.

Furthermore Tolopka fails to teach or render obvious the features of the second data user sending an empty form including a policy to the first data user requesting the personally identifiable information, and wherein the first data user checks the policy included with the empty form to determine if disclosure of the personally identifiable information is permitted based on the policy included with the empty form and the rules regarding the collected data. To the contrary, Tolopka merely teaches that a user may edit a data structure and store it on a storage medium. Neither Tolopka nor King, either alone or in combination, teach or render obvious such exchange of forms and checking of policies with rules as set forth in claim 3.

In view of the above, Appellants respectfully submit that the alleged combination of King and Tolopka does not teach or render obvious the features of claim

3. Accordingly, Applicants respectfully request that the rejection of claim 3 under 35 U.S.C. § 103(a) be withdrawn.

VII. Rejection under 35 U.S.C. § 103(a) Based on King and Gifford

The Office Action rejects claims 19, 25-26, 28, 31-32, 34, and 37-38 under 35 U.S.C. § 103(a) as being allegedly unpatentable over King in view of Gifford (U.S. Patent No. 5,614,927). This rejection is respectfully traversed for at least the same reasons as set forth above with regard to the 35 U.S.C. § 102(e) rejection based on King. That is, King does not teach or render obvious the features discussed above with regard to independent claims 1, 27, and 33 from which claims 19, 25-26, 28, 31-32, 34, and 37-38 depend, respectively. Moreover, Gifford does not provide any teaching technical rationale to implement the features of the independent claims that are missing from King as noted above.

Gifford is directed to a system and method for protecting a database against deduction of confidential attribute values therein. A memory is provided for storing the database and a processor is provided for processing the database. Using the processor, the database is electronically partitioned into public attributes, containing non-confidential attribute values, and private attributes, containing private attribute values. The processor is then used to electronically process the private attribute values to reduce any high correlation between public attribute values and private attribute values.

Gifford is cited by the Office Action as allegedly teaching depersonalization of objects (see July 23, 2008 Office Action, pages 5-6) at column 8, lines 1-8. Column 8, lines 1-8 teaches that after partitioning a database, the correlation between public attributes and private attributes is reduced by camouflaging some highly correlative public attribute values and outright removing some tuples containing highly correlative public attribute values which are difficult to camouflage.

With regard to claims 19, 28, and 34, neither King nor Gifford, either alone or in combination, teach or render obvious the features of transforming, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user. Camouflaging the

correlation between a public attribute and a private attribute in a partitioned database does not teach or suggest transforming, based on rules, personally identifiable information into a *depersonalized format prior to providing the personally identifiable information to the second data user*. All that Gifford teaches is that the link between one attribute and another is camouflaged within a database. Breaking the link between attributes within a database does not cause personally identifiable information that is being sent to a second data user to be depersonalized prior to the sending of that information to second data user. To the contrary, it merely prevents someone from accessing the database and to obtain private attributes by following the link from a public attribute to the private attribute. Furthermore, King does not teach or provide any technical rationale to depersonalize information being provided to the content server, as recognized by the Office Action (Office Action, page 7, item 22). Thus, contrary to the allegations in the Office Action, Gifford does not in fact teach or render obvious the features of claims 19, 28, and 34.

With regard to claims 25, 31, and 37, neither King nor Gifford, either alone or in combination, teach or render obvious the features of the transforming, based on the rules, of the personally identifiable information into a depersonalized format prior to providing the personally identifiable information to the second data user comprises *removing information that relates the personally identifiable information to the data subject in a reversible manner*. Again, merely severing the link between public attributes and private attributes in a database does not cause information to be removed from personally identifiable information that relates the personally identifiable information to a data subject *in a reversible manner* prior to the personally identifiable information being provided to a second data user.

Furthermore, as noted above, the Office Action admits that King does not teach such features either. Thus, any alleged combination of King and Gifford still would not teach or render such features obvious. To the contrary, the combination of King and Gifford would be some concoction primarily as presented by King in which some database somewhere that has private and public attributes has the link between private and public attributes severed. The result of the alleged combination, assuming such a

combination were possible and one were somehow motivated to combine the teachings of the references, *arguendo*, would not be the invention as recited in claims 25, 31, and 37.

Regarding claims 26, 32, and 38, neither King nor Gifford, either alone or in combination, teach or render obvious the features of the transforming, based on the rules, of the personally identifiable information into an anonymized format prior to providing said personally identifiable information to the second data user, ***wherein the anonymized format is a format in which all elements that may allow the personally identifiable information to be related to the data subject are stripped off in a non-reversible manner.*** Again, Gifford only teaches severing the link between public and private attributes within a database such that one cannot use a public attribute to gain access to the private attribute. Gifford does not teach or provide any technical rationale to depersonalize personally identifiable information that is to be provided to a second data user prior to the information being provided to the second data user by stripping off all elements that may allow the personally identifiable information to be related to the data subject.

Furthermore, as noted above, the Office Action admits that King does not teach such features either. Thus, any alleged combination of King and Gifford still would not teach or render such features obvious. To the contrary, the combination of King and Gifford would be some concoction primarily as presented by King in which some database somewhere that has private and public attributes has the link between private and public attributes severed. The result of the alleged combination, assuming such a combination were possible and one were somehow motivated to combine the teachings of the references, *arguendo*, would not be the invention as recited in claims 26, 32, and 38.

In view of the above, Applicants respectfully submit that the alleged combination of King and Gifford does not teach or render obvious the features of claims 19, 25-26, 28, 31-32, 34, and 37-38. Accordingly, Applicants respectfully request that the rejection of claims 19, 25-26, 28, 31-32, 34, and 37-38 under 35 U.S.C. § 103(a) set forth in the Office Action be withdrawn.

VIII. Newly Added Claims 39-40

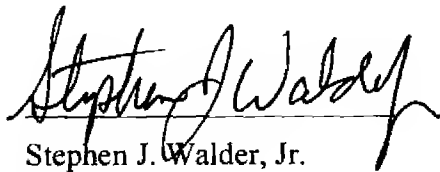
Claims 39-40 are added to recite additional features of the present invention. Neither King, Tolopka, nor Gifford, either alone or in combination, teach or render obvious the specific methods recited in claims 39-40 at least by virtue of their dependencies and further by virtue of the specific features recited in these claims. Prompt and favorable consideration of claims 39-40 is respectfully requested.

IX. Conclusion

It is respectfully urged that the subject application is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: March 16, 2010



Stephen J. Walder, Jr.

Reg. No. 41,534

WALDER INTELLECTUAL PROPERTY LAW, P.C.

17330 Preston Road, Suite 100B

Dallas, TX 75252

(972) 380-9475

ATTORNEY FOR APPLICANTS